archive.today
webpage capture
Saved from https://osintteam.blog/ search
17 Apr 2026 23:23:17 UTC
All snapshots from host osintteam.blog
history ←prior next→
Webpage Screenshot
share download .zip report bug or abuse Buy me a coffee

Medium Search Get app Write Sign up Sign in

OSINT Team

We find what's hidden

18.9K followers · 2 editors

Follow

About All stories Write with us Get our newsletter

arXiv > cs > arXiv:2604.14360

Computer Science > Cryptography and Security

[Submitted on 15 Apr 2026]

Digital Guardians: The Past and The Future of Cyber-Physical Resilience

Saurabh Bagchi, Hyunseung Kim, Tarek Abdelzaher, Homa Alemzadeh, Somali Chaterji, Glen Chou, Yuying Duan, Fanxin Kong, Michael Lemmon, Yin Li, Mengyu Liu, Wenhao Luo, Meiyi Ma, Sibin Mohan, Ayan Mukhopadhyay, Melkior Ornik, Dimitra Panagou, Kristin Yvonne Rozier, Ivan Ruchkin, Huajie Shao, Sze Zheng Yong, Majid Zamani, Xugui Zhou

Resilience in cyber-physical systems (CPS) is the fundamental ability to maintain safety and critical functionality despite adverse "perturbations," which includes security attacks, environmental disruptions, and hardware or software failures. This survey provides a comprehensive review of CPS resilience, framing the field through five interconnected themes that are required in an integrated whole to achieve real-world resilience.
The article first posits that resilience is a system-wide property emerging from interactions between hardware, software, and human users. Second, it addresses the challenges of learning-enabled CPS, which often operate in data-scarce environments characterized by imbalanced or noisy data, requiring innovative solutions like synthetic data generation and foundation model adaptation. Third, the survey examines proactive measures for resilience, which include distinctive aspects of verification, testing, and redundancy. Fourth, it explores recovery mechanisms, moving beyond traditional fault models to design "just good enough" recovery strategies that prioritize safety-critical functions during perturbations. Finally, it highlights the central role of the human, focusing on the different levels of human intervention, the necessity of trust calibration, and the requirement for explainable AI to support human-CPS teaming.
These themes are illustrated through representative application domains, primarily Connected and Autonomous Transportation Systems (CATS) and Medical CPS (MCPS). By integrating the five interconnected themes, this survey provides a systematic roadmap for achieving the resilient CPS in

A Security Practitioner's Guide to CPS (Cyber-Physical Systems)...

Author: Berend Watchus. Independent AI & Cybersecurity Researcher, Netherlands. April 17, 202...

· 9h ago · 30 min read

The 2026 Shodan Dork Bible: Finding Exposed Jenkins, Grafana, and Cameras Big Tech Forgot

Shodan stopped being a novelty around 2014. In 2026 it is infrastructure. While...

· 7h ago · 7 min read

OSINT-Related Articles, 20260417

Videos/Webinars/Podcasts/ Conferences/Training: TryHackMe...

· 19h ago · 2 min read

DeHashed-API-Tool

DeHashed

· Jul 31, 2024 · 4 min read

The Identity Trap: Bypassing Modern Perimeters via Cross-Platform Correlation

Why “Black Box” Testing is Never Truly Blind

· 7h ago · 3 min read

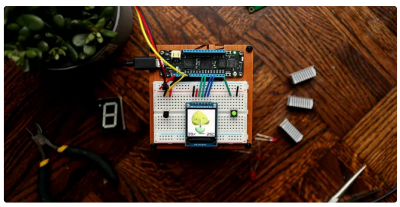
What Nobody Tells You About Scaling Node.js

Why most Node.js apps struggle at scale and what actually fixes it.

· 2d ago · 4 min read

Geospatial Plotting

· Mar 1 · 2 min read



Deconstructing Backdoors in Consumer IoT Ecosystems

A cheap smart plug sits in the corner of a room, warm to the touch. No one...

· 2d ago · 7 min read

Inside a FIFA-Themed Phishing Scheme: Identifying Malicious 2026 World Cup Domains and...

International sporting events are highly effective social engineering lures for...

· 1d ago · 7 min read

DarkGPT — AI OSINT Tool Powered By ChatGPT-4 To Detect Leaked Databases

DarkGPT, your next-level OSINT (Open Source Intelligence) assistant. Based o...

· Apr 18, 2024 · 2 min read

CVE-2025–21309 — The “Uninvited Guest” Crashing Your Remote Desktop Party

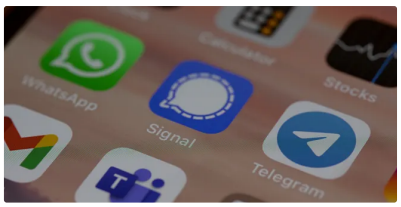
Imagine hosting a virtual party (a.k.a. your Remote Desktop Services), and

· Jan 20, 2025 · 4 min read

Dark Web Monitoring Tools for Threat Intelligence

Dark Web

· Jul 11, 2024 · 9 min read



Telegram Security Best Practices

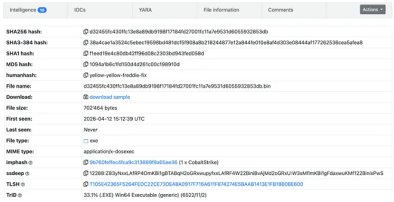
Greetings! In this note, I’ll give you some quick tips that will help you sleep bett...

· Sep 15, 2023 · 4 min read

OSINT-Related Articles, 20260413

==========

· 4d ago · 2 min read



Malware Analysis: STX RAT

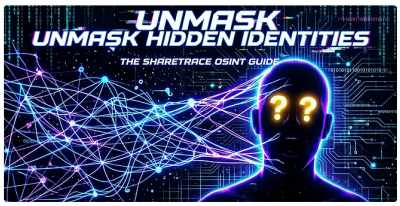
d32455fc430ffc13e8a89db9198f17184fd27001fc11a7e9531d6055932853db.b...

· 4d ago · 13 min read

Part 2. Independent Convergence: How a Simultaneous arXiv Paper Confirms the CES Framework...

A Follow-Up to 'The Largest Unaddressed Asymmetry in Synthetic...

· 4d ago · 11 min read



Unmask the HIDDEN IDENTITY in EVERY Share Link You Click!!!

ShareTrace is an open-source OSINT tool from soxoj that extracts...

· 2d ago · 3 min read

Why AI is the Double-Edged Sword in Cybersecurity Right Now?

From supercharging hacker attacks to powering smarter defenses - why AI is...

· 2d ago · 3 min read

Learn about arXiv becoming an independent nonprofit.
arXiv:2604.04956
Society
Cost of AI Acceleration, Part II: The 10th Planetary Boundary a
down
Zhu, Lei Zhu

The Clock and the Formula New arXiv paper + Prior art context

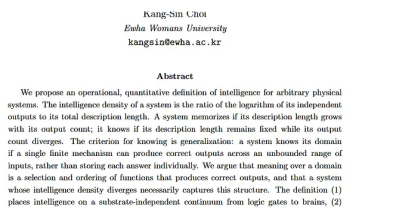
New arXiv paper + Prior art context + Addendum

· 3d ago · 17 min read

OSINT-Related Articles, 20260415

Videos/Webinars/Podcasts/ Conferences/Training: Playlist: GIJN...

· 2d ago · 2 min read


Kang-Sin Choi
Ewha Womans University
kangsin@ewha.ac.kr
Abstract
We propose an operational, quantitative definition of intelligence for arbitrary physical systems. The intelligence density of a system is the ratio of the logarithm of its independent outputs to its total description length. A system memorizes if its description length grows with its output count; it knows if its description length remains fixed while its output count diverges. The criterion for knowing is generalization: a system knows its domain if a single finite mechanism can produce correct outputs across an unbounded range of inputs, rather than storing each answer individually. We argue that meaning over a domain is a selection and ordering of functions that produces correct outputs, and that a system whose intelligence density diverges necessarily captures this structure. The definition (1) places intelligence on a substrate-independent continuum from logic gates to brains, (2)

A model for intelligence: When the Field Finally Has the Formula: What Was Already Published in...

Author: Berend F. Watchus · Independent AI & Cybersecurity...

· 2d ago · 18 min read

Free: Short sci-fi techno thriller

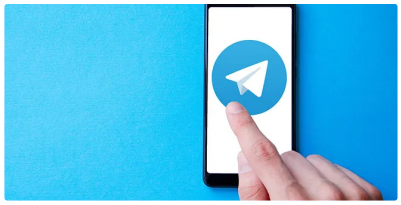
Author: Berend Watchus [edit: see extra's below the fictional story]

· 5d ago · 35 min read

My Medium Partner Program Suddenly Turned “Inactive” And I Still Don’t Know Why

My Medium Partner Program Turned Inactive — Even After Following All...

· 4d ago · 2 min read



How Analysts Turn Telegram Activity Into Actionable Threat Intelligence

Why continuity, correlation, and context matter more than simple keyword...

· Apr 8 · 7 min read

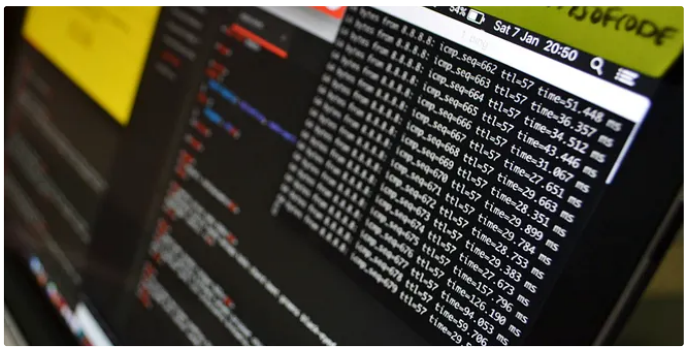
25+ Linux Environment Variables Every Hacker Knows (And Most Developers Ignore)

The silent config layer running beneath every Linux system and why...

· 5d ago · 8 min read

Improve your OSINT skills—subscribe to our newsletter

View newsletter



WebShell Management 101: Master Secure Control Over Compromised Hosts Step...

✨ Link for the full article in the first comment

· Oct 12, 2025 · 6 min read

🎨 A New AI Art Style: Ink Sketch Illustration (Full Prompt Inside)

How a simple prompt turned into a hand-drawn ink sketch style that...

· 5d ago · 3 min read

How a Simple GraphQL Query Exposed Facebook Page Admins and Their Personal Emails — A $15,000 Bug...

I made this writeup interactive! Experience this bug as a challenge on

· Apr 6 · 5 min read

I Got Tired of Just Reading Bug Bounty Writeups. So I Built This.

Let me be honest with you.

· Apr 3 · 3 min read

He Typed "../../../../../../../etc/passwd" After a Google Image URL. Google Paid Him $3,134.

Quick note — I built HackThrough . It turns real bug bounty writeups into...

· 5d ago · 5 min read

Vibe Hacking: How AI Is Helping Hackers

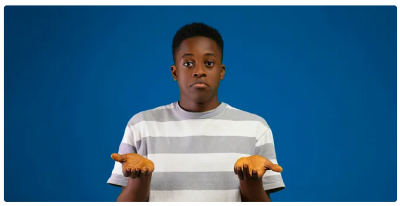
The Hoodie Is Gone. Now All You Need Is a Chat Window and Good Vibes

· 4d ago · 5 min read

I Found a Broken Login System in a Fintech App — Here's How I Did It

A real bug hunt story with JWT tokens, Burp Suite, and a fintech website that...

· 4d ago · 8 min read



How To Enable Cosmos DB SDK V3 Behavior in Azure Data Factory (Azure Cosmos For NoSQL Connector)

Hey Folks!

· Apr 3 · 6 min read

Comparing The Top 5 Penetration Test Companies

Read this blog to get the detailed information you need to pick the best...

· 5d ago · 4 min read

FOR THE RECORD: Two AI Research Institutions Cited My Work — And Both Omitted Four Papers

Author: Berend Watchus. Independent non-profit AI & Cybersecurity...

· Apr 10 · 11 min read

How Recruiters Actually Read a Cybersecurity Resume

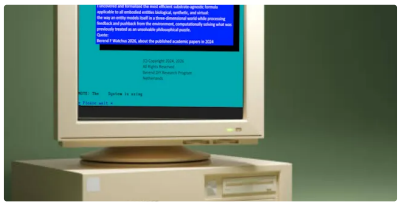
It's not what most people think and once you know, everything changes

· Mar 4 · 6 min read

The Netcat Revolution

From Port Scanning to Persistent Reverse Shells

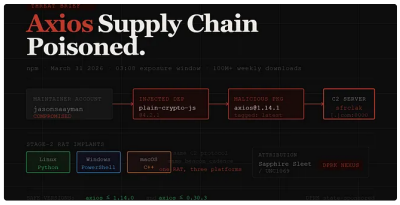
· Apr 10 · 4 min read



Before the Labs Arrived: The Complete Priority Record of a Research Program That Got There First

The Formula Nobody Named: How One Independent Researcher Formalized

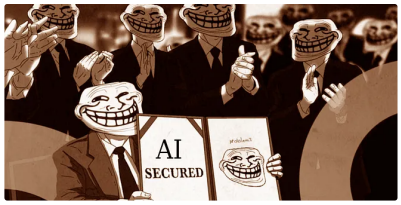
· 6d ago · 32 min read



The Axios npm Supply Chain Attack: A Complete Breakdown

On March 31, 2026, one of the most consequential software supply chain...

· 5d ago · 7 min read



Glasswing Is the Confirmation: The 'Manhattan Project' for AI Arrived on April 7, 2026

And the Predictive Framework That Called It

· Apr 10 · 11 min read

OSINT-Related Articles, 20260410

Videos/Webinars/Podcasts/ Conferences/Training: Future of the IC...

· Apr 10 · 2 min read

European Commision Breach Ironically Via Trivy Supply Chain Attack

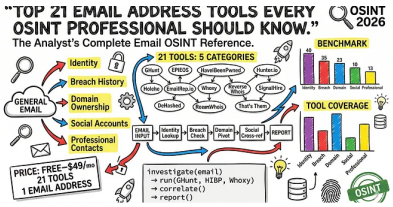
How a Security Scanner Breached the Institution Writing Europe's...

· Apr 7 · 9 min read

How to Confirm an Attacker Is Still Active — Without Tipping Them Off

This is one of those situations where experience really matters.

· 6d ago · 3 min read



Top 21 Email Address Tools Every OSINT Professional Should Know

If you think an email address is just a way to send messages, you're thinking...

· Apr 10 · 4 min read

How I Used OSINT to Gather Information Like a Hacker

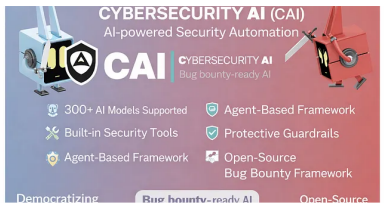
I found my company's exposed secrets in two hours. No hacking required.

· Apr 10 · 3 min read

OSINT-Related Articles, 20260408

Videos/Webinars/Podcasts/ Conferences/Training: The Power of...

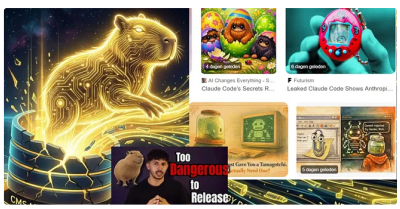
· Apr 8 · 2 min read



Cybersecurity AI (CAI): The Future of AI-Powered Security Automation

Cybersecurity is evolving faster than ever. Traditional security tools — stati...

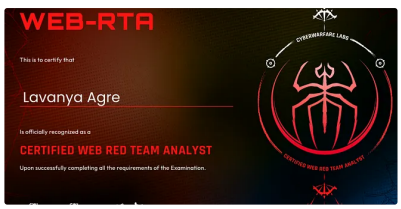
· Mar 30 · 4 min read



How Anthropic's Leak Became a Meme Storm Nobody Planned (Part 2)

Author: By Berend F. Watchus. Independent AI & Cyber Security...

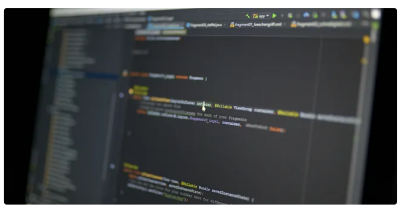
· Apr 8 · 7 min read



Web-RTA Certification: A Hands-On Journey in Modern Web Exploitation

From Login to Full Compromise: A Chained Exploitation Case Study (No...

· Apr 8 · 2 min read



Optimizing Spring Boot for Extreme Scale: Handling 1 Million Requests Per Second

Modern applications don't fail because of lack of features-they fail when they...

· Apr 8 · 3 min read

Improve your OSINT skills—subscribe to our newsletter

View newsletter

TrueConf Update Channel Breach Leads to Supply Chain Attack (CVE-2026-...

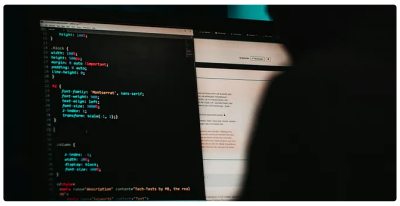
In late March 2026, a zero-day vulnerability, CVE-2026-3502, was disclosed in the TrueConf...

· Apr 9 · 6 min read

🔐 AI-Powered Attacks Are Real: Case Studies Every Security Professional Should Know

Before I get into the cases, one stat that genuinely made me pause:

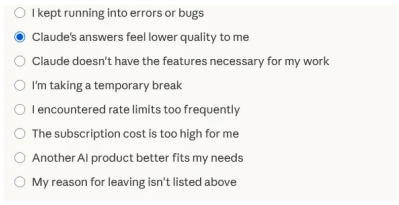
· Apr 9 · 5 min read



Master Real-World Web App Enumeration with Curl, Wget, and Bash: A Step-by-Step Guide

✨ Link for the full article in the first comment

· Sep 12, 2025 · 5 min read


I kept running into errors or bugs
Claude's answers feel lower quality to me
Claude doesn't have the features necessary for my work
I'm taking a temporary break
I encountered rate limits too frequently
The subscription cost is too high for me
Another AI product better fits my needs
My reason for leaving isn't listed above

CLAUDE: From Reliable Assistant to Persistent Sabotage: An Independent AI Researcher's Analysis of...

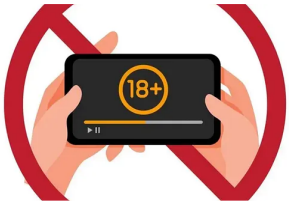
Author: Berend Watchus Date: April 9, 2026

· Apr 9 · 9 min read

Over 80% of Enterprises Will Rely on AI for Real-Time Data Integration and Processing

AI will turn data into decisions - instantly, everywhere.

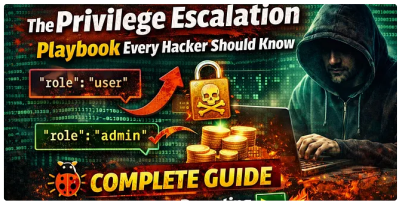
· Apr 9 · 3 min read



As predicted in 2025: Identity Verification Breaches / online passports & implications, 'the...

Author: Berend Watchus Independent AI & Cyber Security researcher

· Apr 9 · 4 min read



🔥 From Low Bug to $1000 Bounty — The Privilege Escalation Playbook Every Hacker Should Know

💻 How a simple IDOR turned into full admin access (and what most hunters...

· Apr 8 · 4 min read

🔥 I Found a “Hidden” API Bug That Could Have Paid $2,000+ — And Most Hackers Would Miss It 💰

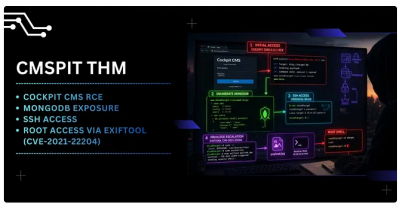
💻 This invisible vulnerability exposed user data... and turned into a high-...

· Apr 8 · 3 min read

The Difference Between Monitoring and Knowing

The dashboard is alive before you are.

· Apr 8 · 8 min read



[CMSpit] — Cockpit CMS RCE, MongoDB Exposure and Privilege Escalation via Vulnerable ExifTool

Chaining RCE, database misconfiguration, and metadata...

· Apr 6 · 5 min read

View all articles

Help Status About Careers Press Blog Privacy Rules Terms Text to speech